# Tätigkeitsbericht 2013

Datenschutzbeauftragter
des Kantons Luzern

KANTON LUZERN

Datenschutzbeauftragter | datenschutz.lu.ch

# Inhalt



# Vorwort

Der Datenschutzbeauftragte hat gemäss § 23 Abs. 1 lit. k DSG[1] dem Regierungsrat jährlich Bericht über seine Tätigkeit zu erstatten und stellt der Aufsichts- und Kontrollkommission des Kantonsrates eine Kopie zu; der Bericht wird öffentlich zugänglich gemacht.

Der vorliegende Bericht erstreckt sich über den Zeitraum vom 1. Januar 2013 bis 31. Dezember 2013. Das Berichtsjahr war – bei unverändert sehr angespannten Personalressourcen – durch eine im Vergleich zum Vorjahr wiederum klare Erhöhung der Geschäftsfälle gekennzeichnet (+17%). Die prekäre Ressourcensituation mit insgesamt 90 Stellenprozenten (davon 50% juristisch), aufgeteilt auf zwei Personen, führt weiterhin zu einer nicht optimalen Erreichbarkeit der Datenschutzstelle, zu einer Erschwerung der zeitnahen Erledigung der Anfragen sowie zu Verzögerungen bei der Mitarbeit in Projekten.

Folge dieser prekären Ressourcensituation ist, dass die gesetzlichen Aufgaben wiederum nicht vollumfänglich wahrgenommen werden konnten und sich die Lage von Jahr zu Jahr verschärft.

[1] Gesetz über den Schutz von Personendaten (Datenschutzgesetz) vom 2. Juli 1990, SRL Nr. 388

Diese Situation ist auch im Hinblick auf die internationalen Verpflichtungen der Schweiz im Bereich des Datenschutzes unverändert kritisch.

Das Berichtsjahr war geprägt durch

- die Beratung kantonaler und kommunaler Stellen sowie Privater,
- die Begleitung grösserer kantonaler Projekte,
- die Durchführung einer Datenschutzkontrolle der Anwendung NEST (LuTax),
- das Ausarbeiten von Vernehmlassungen in verschiedenen Gesetzgebungsverfahren des Kantons und des Bundes
- vereinzelte Vorträge und Schulungen (Datenschutzsensibilisierung),
- die Beantwortung von Medienanfragen sowie
- aufsichtsrechtliches Einschreiten bei Datenschutzverletzungen.

Es lässt sich positiv festhalten, dass das Interesse am Datenschutz in den Gemeindeverwaltungen (+ 63% Anfragen gegenüber Vorjahr) sowie in der Bevölkerung (+ 26% Anfragen) stetig zunimmt und die Anfragen vermehrt über das Internet, nämlich via Kontaktformular (53) oder E-Mail (119) an uns gelangen. Von den insgesamt 273 Anfragen wurde jedoch in 94 Fällen auch das bewährte Mittel Telefon verwendet, während lediglich 7 briefliche Anfragen an uns gelangten.

Im nachfolgenden Text werden die beiden Begriffe *Datenschutzbeauftragter* und *Datenschutzgesetz* des *Kantons Luzern* oft verwendet. Damit der Text aufgrund dieser häufigen Begriffsverwendungen nicht unnötig in die Länge gezogen wird, sind die Begriffe «Datenschutzbeauftragter» mit DSB und «Datenschutzgesetz des Kantons Luzern» mit DSG abgekürzt.

Dr. iur. Reto Fanger, Rechtsanwalt
Datenschutzbeauftragter des Kantons Luzern

# A. Gesetzlicher Auftrag

Der Auftrag und die Aufgaben des DSB sind in den §§ 22 f. DSG verankert. Diese lauten wie folgt:

§ 22 Aufsicht

1 Der Regierungsrat wählt als kantonale Aufsichtsstelle einen Beauftragten für den Datenschutz. Die Wahl bedarf der Genehmigung durch den Kantonsrat.

2 Der Beauftragte ist fachlich selbständig und unabhängig; administrativ ist er der Staatskanzlei zugeordnet.

3 Die dem Gesetz unterstellten Gemeinwesen können eine eigene Aufsichtsstelle schaffen. Der Beauftragte für den Datenschutz übt in diesem Fall die Oberaufsicht aus.

§ 23 Aufgaben

1 Der Beauftragte für den Datenschutz

a. überwacht die Einhaltung der Vorschriften über den Datenschutz,

b. berät die verantwortlichen Organe in Fragen des Datenschutzes und der Datensicherung,

c. erteilt den betroffenen Personen Auskunft über ihre Rechte,

d. vermittelt zwischen Organen und Personen in allen Anständen über den Datenschutz, namentlich bei Begehren um Auskunft, Berichtigung und Unterlassung,

e. reicht in hängigen Verfahren auf Ersuchen von entscheidenden Organen oder Rechtsmittelbehörden Stellungnahmen zu Datenschutzfragen ein,

f. orientiert die Organe über wesentliche Anliegen des Datenschutzes,

g. sorgt für die Instruktion der Mitarbeiter von Organen über den Datenschutz,

h. kontrolliert im Voraus Bearbeitungsmethoden, welche die Persönlichkeit einer grösseren Anzahl von Personen verletzen könnten,

i. veröffentlicht Stellungnahmen,

j. arbeitet mit den Kontrollorganen der anderen Kantone, des Bundes und des Auslandes zusammen,

k. erstattet dem Regierungsrat jährlich Bericht über seine Tätigkeit und stellt gleichzeitig der Aufsichts- und Kontrollkommission des Kantonsrats eine Kopie zu; der Bericht wird öffentlich zugänglich gemacht.

2 Er führt für den Kanton das Register über die Datensammlungen.

# B. Statistische Angaben

Die Dienstleistungen des DSB im Berichtsjahr können wie folgt zusammengefasst werden:

| **Dienstleistungen** | 2009 | 2010 | 2011 | 2012 | **2013** | Entwicklung (2012 – 2013) |
|---|---|---|---|---|---|---|
| 1. Auskunft | | | | | | |
| Anfragen Gemeinden | 25 | 40 | 40 | 30 | **49** | + 63% |
| Anfragen Kanton* | | | | *77* | **70** | – 9% |
| Anfragen Private* | | | | 122 | **154** | + 26% |
| Total Auskunft | 139 | 148 | 148 | 229 | **273** | **+ 19%** |
| Anfragen ohne Ablage (einfache schriftl. Auskünfte) | 108 | 125 | 133 | 198 | **– **** | –** |
| Anfragen mit Ablage (komplizierte Dossiers) | 31 | 23 | 15 | 31 | **– **** | –** |
| *wovon betreffend Bereich Informatik* | | *19* | *8* | *18* | **12** | *– 33%* |
| *wovon betreffend Bereich Polizei* | | *10* | *7* | *15* | **6** | *– 60%* |
| *wovon betreffend Bereich Bildung** | | *10* | *7* | *33* | **33** | *+/– 0%* |
| *wovon betreffend Bereich Soziales** | | *10* | *7* | *34* | **66** | *+ 94%* |
| *wovon betreffend Bereich Privat** | | *10* | *7* | *19* | **40** | *+ 111%* |
| *wovon betreffend Bereich Gesundheit* | | *25* | *16* | *26* | **19** | *– 27%* |
| *wovon betreffend verschiedene andere Bereiche (Diverse)* | | *54* | *77* | *84* | **97** | *+ 15%* |
| 2. Projekte und Weiterbildung | | | | | | |
| Mitarbeit in Projekten | 3 | 6 | 5 | 20 | **22** | + 10% |
| Leitung von Projekten | 0 | 0 | 0 | 0 | **0** | – |
| Geleitete Ausbildungsveranstaltungen | 1 | 0 | 0 | 3 | **3** | +/– 0% |
| Gehaltene Vorträge | 3 | 2 | 3 | 0 | **3** | + 300% |
| Total Geschäftsfälle | 145 | 156 | 158 | 257 | **301** | **+ 17%** |

* neue Rubriken seit 2012
** mit Einführung der Geschäftsverwaltungsanwendung Konsul im Berichtsjahr wird nicht mehr zwischen Anfragen mit/ohne Ablage unterschieden

Im Berichtsjahr haben – abgesehen von der generellen Zunahme in den meisten erhobenen Bereichen – vor allem die Anfragen in den Bereichen Soziales und Privat sehr stark zugenommen. Eine Abnahme der Anfragen konnten wir in den Bereichen Gesundheit, Polizei und Informatik feststellen. Informatik-Anfragen begleiten wir vermehrt in grösseren Projekten, wo wir eine Zunahme gegenüber dem Vorjahr von 10% ausmachen können.

Im Rahmen eines Mehrjahresvergleichs fällt auf, dass die jährliche Steigerung der Geschäftslast kontinuierlich ausfällt, hat doch seit 2010 die Anzahl Anfragen um 85%, die Anzahl der Projekte um 266% und die Anzahl der Geschäftsfälle insgesamt um 93% zugenommen.

Noch markanter fällt ein Fünfjahresvergleich der aktuellen Zahlen mit dem Jahr 2009 aus: Die Anfragen haben gegenüber 2009 um 96%, die aufwändigen Projekte um 633% und die Geschäftsfälle insgesamt um 107% zugenommen.

# C. Anfragen und Gesuche

Nachfolgend werden exemplarisch bestimmte Anfragen, Gesuche und Projekte erwähnt, die im Verlaufe des Berichtsjahres behandelt wurden:

## 1. Bereich Polizei

### Keine öffentlichkeitsrelevanten Anfragen

Zwar wurden auch im Berichtsjahr mehrere Anfragen im Bereich Polizei gestellt. Von öffentlichem Interesse war jedoch keine dieser Anfragen.

## 2. Bereich Gemeinden

### Einbürgerungsgesuche

Einbürgerungsgesuche werden je nach Gemeinde unterschiedlich veröffentlicht, beispielsweise im Rahmen einer schriftlichen «Botschaft zur Gemeindeversammlung», die an alle Haushaltungen der Gemeinde verschickt und gleichzeitig zum Download auf der Website der Gemeinde bereitgestellt wird.

Frage:
Dürfen darin Adressen und Fotos der Gesuchstellenden veröffentlicht werden?
In Bezug auf die Publikation von Gemeindeinformationen gelten folgende Rahmenbedingungen:

a) das Datenschutzreglement der entsprechenden Gemeinde (z.B. Art. 3 «Veröffentlichung von Personendaten») und subsidiär das kantonale DSG.
b) das Bürgerrechtsgesetz (BüG) und die zugehörige Verordnung (BüV) sowie
c) die kommunalen rechtlichen Grundlagen für Publikationen: z.B. «Die direkt betroffene Person muss ihr Einverständnis mit der Publikation schriftlich (E-Mail) einreichen».

Für die Publikation von Einbürgerungsgesuchen gilt daher: Bei der Aktenauflage dürfen schutzwürdige private und öffentliche Interessen nicht gefährdet werden (§ 13 Abs. 5 BüV). Es darf nur eine Zusammenfassung jener Fakten aufgelegt werden, die für den Entscheid wesentlich sind (vgl. Art. 15c BüG). Die Einkommens- und Vermögenssituation gehört nicht dazu. Bei der Veröffentlichung von Daten im Internet sind die Empfehlungen des DSB zu beachten.

Jede Einbürgerung wird publiziert (§ 17 BüV). Die Publikation erfolgt ohne Rechtsmittelbelehrung, wenn eine Gemeindebehörde entschieden hat; ein Rechtsmittel steht hier nicht zur Verfügung.

Im Rahmen eines Einbürgerungsverfahrens dürfen nur jene Daten einer einbürgerungswilligen Person veröffentlicht werden, die für die Einbürgerungsentscheidung wesentlich sind. Bei einer Publikation der Einbürgerungsdaten im Internet ist das Risiko einer Persönlichkeitsverletzung besonders hoch. Es dürfen deshalb nur die für die Identifikation notwendigen Daten im Internet veröffentlicht werden.

Fazit:
Die Gemeinden stellen den Stimmberechtigten eine Weisung (beleuchtender Bericht) zu, die Angaben zu den an der Gemeindeversammlung traktandierten Einbürgerungsgeschäften enthält. Das Material, das die Stimmberechtigten erhalten, darf nur jene Daten enthalten, die nötig sind, um die Kandidatinnen und Kandidaten zu identifizieren. Dies sind Name, Vorname, Geburtsjahr, Adresse und Herkunftsland. Zusätzliche Angaben, wie z.B. die Angabe der Konfession, sind weder geeignet noch erforderlich und haben somit zu unterbleiben. Der Informationsbedarf der stimmberechtigten Bürgerinnen und Bürger ist ausreichend gedeckt, wenn sie Gelegenheit haben, die für ihren Entscheid relevanten Akten vor der Abstimmung in der Gemeindekanzlei einzusehen. Bei der Aktenauflage dürfen aber schutzwürdige private und öffentliche Interessen nicht gefährdet werden (§ 13 Abs. 5 BüV). Unter

Berücksichtigung des Grundsatzes der Verhältnismässigkeit ist nur eine Zusammenfassung jener Fakten aufzulegen, die für die Entscheidung über die Einbürgerung wesentlich sind. Die Einkommens- und Vermögenssituation gehört nicht dazu. Soweit die Weisungen auf der Webseite der Gemeinde aufgeschaltet und damit der allgemeinen Öffentlichkeit zugänglich gemacht werden, sind die Grundsätze für Veröffentlichungen von Einbürgerungsdaten im Internet zu beachten.

### Steuerauskunft

Das Steueramt einer Gemeinde erhält die folgende Anfrage:
Eine Anwältin vertritt eine Exfrau eines Steuerpflichtigen in unserer Gemeinde und ersucht um Steuerauskunft (steuerbares Vermögen und steuerbares Einkommen) für diesen Steuerpflichtigen. Als Interessennachweis legt sie einen Verlustschein infolge Konkurs bei. Offenbar mache der Schuldner (Steuerpflichtige) bei erneuten Betreibungen geltend, dass er nicht zu neuem Vermögen gekommen ist.

Frage:
Darf das Steueramt hier Auskunft geben?

Fazit:
Gemäss § 10 Abs. 1 lit. a DSG braucht es für eine entsprechende Auskunft eine rechtliche Grundlage (lit. b trifft vorliegend nicht zu):

§ 10 Bekanntgeben an Private

1 Unter Vorbehalt besonderer Geheimhaltungspflichten darf ein Organ privaten Personen und Organisationen Personendaten bekanntgeben, wenn a. ein Rechtssatz dazu verpflichtet oder ermächtigt oder b. die betroffene Person eingewilligt hat oder ihre Einwilligung nach den Umständen vorausgesetzt werden kann.

2 Personendaten aus allgemein zugänglichen amtlichen Veröffentlichungen darf ein Organ auf Anfrage in dem Umfang und in gleicher Weise bekanntgeben, wie sie veröffentlicht worden sind.

3 Der Regierungsrat regelt das Bekanntgeben von Personendaten für Adressbücher und andere Nachschlagewerke sowie für Publikationen im Zusammenhang mit andern Vorgängen von allgemeinem Interesse.

Eine entsprechende rechtliche Grundlage für die gewünschte Datenbekanntgabe fehlt vorliegend. Im Gegenteil, setzt doch das kantonale Steuergesetz in § 134 vielmehr eine Geheimhaltungspflicht fest, welche die gewünschte Auskunft an die Anwältin verunmöglicht:

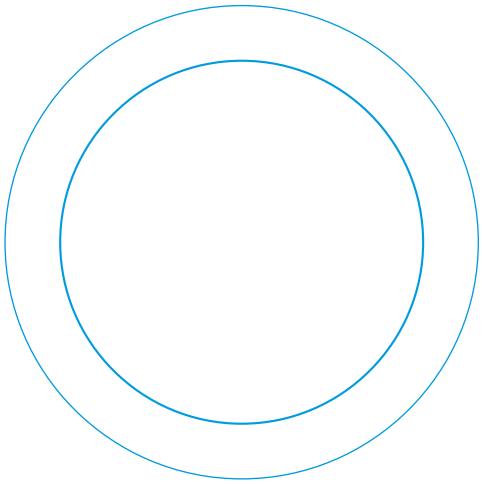
§ 134 Geheimhaltungspflicht

1 Wer mit dem Vollzug dieses Gesetzes betraut ist oder dazu beigezogen wird, muss über Tatsachen, die ihm in Ausübung seines Amtes bekannt werden, und über die Verhandlungen in den Behörden Stillschweigen bewahren und Dritten den Einblick in amtliche Akten verweigern.

2 Eine Auskunft, einschliesslich der Edition von Akten, ist zulässig, wenn dafür eine ausdrückliche gesetzliche Grundlage im Recht des Bundes oder des Kantons besteht. Fehlt eine solche Grundlage, ist eine Auskunft an Verwaltungsbehörden und Gerichte zulässig, soweit sie im öffentlichen Interesse geboten ist.

3 Über Auskunftsbegehren entscheidet das Finanzdepartement endgültig. Es kann für bestimmte Auskünfte generelle Ermächtigungen erteilen oder die Entscheidbefugnis der Dienststelle Steuern des Kantons übertragen.

Eine entsprechende Auskunft wäre allenfalls über ein gerichtliches Verfahren möglich (z.B. vorsorgliche Beweisführung), mit welchem die gerichtliche Edition der gewünschten Unterlagen/Informationen erreicht wird.



### Auskunft in Bezug auf die Krankenversicherungspflicht

Wir haben auch einige Anfragen von Privaten in Bezug auf die Klausel im Formular einer Einwohnerkontrolle erhalten: Das Obligatorium der Krankenpflegeversicherung ist in den Art. 3-7 des Bundesgesetzes über die Krankenversicherung (KVG) verankert. Grundsätzlich haben sich alle Personen in der Schweiz, unabhängig von einer Erwerbstätigkeit, einer anerkannten Krankenversicherung nach KVG anzuschliessen. Die AHV-Zweigstelle hat die Aufgabe, bei allen Einwohnern die Krankenversicherungspolice der Grundversicherung einzufordern und eine Aktenkopie zu erstellen.

Aufforderung der Einwohnerkontrolle:
Wir bitten Sie deshalb, uns eine aktuelle Krankenversicherungspolice von Ihnen / Ihrer Familie einzureichen.

Fazit:
Die Gemeinde hat die Pflicht zu überprüfen, ob die Einwohner über einen entsprechenden Versicherungsschutz gemäss KVG verfügen. Speziell gilt dies in ausserordentlichen Situationen wie z.B. für Sozialhilfebezüger und Neuzuzüger.

A. Gesetzliche Grundlagen
Obligatorische Krankenversicherungspflicht nach KVG:
Art. 3 Versicherungspflichtige Personen
1 Jede Person mit Wohnsitz in der Schweiz muss sich innert drei Monaten nach der Wohnsitznahme oder der Geburt in der Schweiz für Krankenpflege versichern oder von ihrem gesetzlichen Vertreter beziehungsweise ihrer gesetzlichen Vertreterin versichern lassen.
etc.

In Ausführung dazu, siehe die kantonale Vollziehungsverordnung zum Gesetz über die Niederlassung und den Aufenthalt (SRL Nr. 6), insbesondere § 6 Bst. b:

§ 6
Die Gemeinden können im Einwohnerregister folgende zusätzlichen Merkmale führen:
a. berufliche Tätigkeit und Name des Arbeitgebers,
b. Erfüllung der Versicherungspflicht nach den Artikeln 3 ff. des Bundesgesetzes über die Krankenversicherung (KVG) vom 18. März 1949,
c. Zivilschutzpflicht,
d. Personennummer gemäss der Verordnung über das Zentrale Migrationsinformationssystem (ZEMIS-Verordnung) vom 12. April 2006,
e. Hinterlegung Güter- oder erbrechtlicher Dokumente bei der Teilungsbehörde,
f. Mitgliedschaft im Urnenbüro.

Die genannten rechtlichen Grundlagen setzen die Bearbeitung von Personendaten seitens der Wohnsitzgemeinde voraus. Es reicht dabei aber, wenn der Gemeinde der Versicherungsnachweis mit der Vorweisung der Krankenkassen-Karte erbracht wird. Es trifft zu, dass Art. 3 KVG die Bearbeitung von Personendaten seitens der Wohnsitzgemeinde voraussetzt. Die Vorweisung der Krankenkassen-Karte erscheint dabei ein verhältnismässiges Mittel (erforderlich und geeignet). Alternativ dazu kann der notwendige Beweis auch mit einer schriftlichen Bestätigung der Krankenkasse an die Wohnortgemeinde erbracht werden.

## 3. Bereich Bildung

### Bekanntgabe von Personendaten von Lehrern durch den Gemeinderat

Ausgangslage:
Der Gemeinderat einer kleineren Gemeinde verschickte einen Brief mit Angaben über verschiedene Kategorien von Lehrpersonen – Angaben der Pensen, Jahreslöhne, angebliche Ausbildungsmankos, teilweise unter zusätzlicher Angabe angeblicher charakterlicher oder angeblicher beruffli-

cher Schwächen – an einen sehr breiten Adressatenkreis (einzelne Regierungsräte, Parteipräsidien einzelner Parteien, Fraktionspräsidien einzelner Parteien, eine Kantonsrätin sowie die Finanzvorsteher aller Luzerner Gemeinden). Einige Wochen später wurde der Brief in einem Zeitungsartikel thematisiert und uns unmittelbar darauf von dritter Seite zur Beurteilung vorgelegt.

### Rechtliche Beurteilung

Personendaten (§ 2 Abs. 1 Datenschutzgesetz, DSG):
Bei den im erwähnten Schreiben aufgeführten Informationen handelt es sich zu einem grossen Teil um Personendaten, da diese – insbesondere in einer kleinen Gemeinde mit einer entsprechend kleinen Schulorganisation – ohne weiteres teilweise bereits aufgrund der Funktionsangaben sowie überdies noch in Verbindung mit weiteren charakteristischen Zuschreibungen bestimmten Lehrpersonen zugeordnet werden können.

Besonders schützenswerte Personendaten (§ 2 Abs. 2 DSG):
Da einzelne Lehrpersonen nicht nur beruflich, sondern auch charakterlich umschrieben werden, handelt es sich teilweise gar um besonders schützenswerte Personendaten.

Bearbeiten von Personendaten (§ 2 Abs. 4 DSG):
Das Schreiben des Gemeinderates ist als Datenbekanntgabe und damit als ein Bearbeiten von Personendaten (teilweise von besonders schützenswerten Personendaten) im Sinne des Datenschutzgesetzes einzustufen. Überdies stellen auch das Erheben, Beschaffen und Verwenden von Personendaten durch den Gemeinderat bzw. die zuständigen Schulorgane bis hin zur Bekanntgabe an den Schulverwalter datenschutzrelevante Datenbearbeitungen dar.

Grundsätze des Bearbeitens von Personendaten (§ 4 DSG):
Die Datenbekanntgabe durch den Gemeinderat ist weder als rechtmässig (Abs. 1) noch als verhältnismässig (Abs. 3) einzustufen und verstösst auch gegen das Zweckbestimmungsprinzip. Ob das Gebot der Datenrichtigkeit (Abs. 2) erfüllt ist, lässt sich zur Zeit nicht beurteilen. Abgesehen davon ist auch fraglich, ob gewisse Informationen überhaupt gesammelt bzw. an den Schulverwalter und/oder die übrigen Gemeinderäte weitergegeben werden dürfen. Insgesamt verstossen damit der Gemeinderat und allenfalls auch die Schulbehörden gegen das Datenschutzgesetz.

Verantwortlichkeit für Datenbearbeitung gemäss § 6 DSG:
Die Verantwortlichkeit in Bezug auf diese Datenschutzverletzungen liegen hinsichtlich der Datenbekanntgabe an die Adressaten des Schreibens beim Gemeinderat; hinsichtlich der internen Datenbearbeitung von der Schule über den Schulverwalter bis zum (Gesamt-)Gemeinderat ist die Verantwortlichkeit noch genauer zu klären.

## 4. Bereich Gesundheit

### Mein online Spitaldossier

Aufgrund verschiedener Medienanfragen wurden wir im Berichtsjahr im Verlauf des Monats Mai auf das Pilotprojekt «Mein online Spitaldossier» der HNO-Klinik Luzern des Luzerner Kantonsspitals (LUKS) aufmerksam gemacht, welches offenbar seit anfangs Mai in Betrieb war. Aufgrund der Projektbezeichnung wie auch der entsprechenden Beschreibung auf der Website der HNO-Klinik war ersichtlich, dass es sich dabei um ein elektronisches Patientendossier mit Webzugang der teilnehmenden Patienten handelt. Da Gesundheitsdaten besonders schützenswerte Personendaten darstellen und somit besonders sensitiv sind, wurden die Projektverantwortlichen aufgefordert die rechtlichen Rahmenbedingungen dieses Pilotprojekts zu nennen und die entsprechenden Unterlagen zur Prüfung der datenschutzrechtlichen Zulässigkeit des Projekts offenzulegen.

Obwohl es sich beim LUKS um eine seit 2008 selbständige kantonale öffentlich-rechtliche Anstalt mit eigener Rechtspersönlichkeit handelt, steht diese Form der Rechtspersönlichkeit der Anwendbarkeit des Informatikgesetzes (in dessen Rahmen auch datenschutzrechtliche Fragen im Zusammenhang mit der kantonalen IT-Infrastruktur geregelt sind) wie auch des kantonalen Datenschutzgesetzes vorliegend nicht entgegen, die datenschutzrechtliche Aufsicht durch den DSB ist gewährleistet.

Zu prüfen war in der Folge, ob die datenschutzrechtlichen Anforderungen des Informatikgesetzes bezüglich zentraler Datenbanken, Auslagerung (Outsourcing) und Abrufverfahren sowie überdies generelle datenschutzrechtliche Aspekte erfüllt waren.

Nach Sichtung der zugestellten Unterlagen stellte sich heraus, dass es sich bei «Mein online Spitaldossier» nicht um eine Auslagerung (Outsourcing) von Informatikmitteln oder Informatikdienstleistungen und auch nicht um eine zentrale Datenbank im Sinne des Informatikgesetzes handelte. Allerdings war zunächst noch unklar, ob von einem Abrufverfahren im Sinne von § 3 Abs. 7 des Informatikgesetzes auszugehen sei.

Anlässlich einer Sitzung mit den Projektverantwortlichen sowie nach Sichtung weiterer Unterlagen konnten diverse offene Fragen geklärt werden, unter anderem betreffend dem mittels SMS-Code gesicherten Zugang zum Spitaldossier, der verschlüsselten HTTPS-Verbindung sowie den Möglichkeiten des Benutzers zur individuellen Bestimmung der Zugriffsberechtigungen. Neben den erwähnten datensicherheitstechnischen Aspekten, wurden an dieser Sitzung die aus datenschutzrechtlicher Sicht relevanten Gesetzesbestimmungen und die vertraglichen Rahmenbedingungen des Projekts angesprochen.

Nachdem eine befristete Absichtserklärung (Letter of Intent, LOI) zwischen den projektbeteiligten Parteien automatisch per 30. Juni 2013 ausgelaufen war und anschliessend kein Hauptvertrag abgeschlossen worden war, wurden die Projektverantwortlichen im August des Berichtsjahres aufgefordert, diesen Umstand zu beheben und mit den übrigen projektbeteiligten Parteien eine schriftliche Leistungsvereinbarung abzuschliessen, welche mindestens folgende Punkte regelt:

a. Struktur der zentralen Datenbank,
b. Inhalt der Datenbank insbesondere in Bezug auf Personendaten,
c. verwendete Techniken, einschliesslich Entwicklung und Wartung,
d. Zugriffsverwaltung,
e. Sicherheits- und Datenlöschkonzept,
f. Standort der Hardware,
g. Kontrollrechte und -pflichten,
h. Verantwortlichkeiten.

## 5. Bereich Soziales

### Bin ich auf der schwarzen Liste der säumigen Krankenkassenprämienzahler?

Eine private Person stellte uns folgende Frage:
Wie muss ich vorgehen, um zu erfahren, ob ich auf der «schwarzen Liste der säumigen Krankenkassenprämienzahler» eingetragen bin?

Fazit:
Bei der Ausgleichskasse Luzern kann gestützt auf §15 DSG Auskunft verlangt werden, ob man als Betroffene / Betroffener in der Liste erfasst ist.

§ 15 Auskunft
1 Jede Person kann mündlich oder schriftlich Auskunft verlangen a. beim Organ, welches das Register führt, über

dessen Inhalt, b. beim Inhaber der Datensammlung, ob über sie Personendaten bearbeitet werden. Sie hat sich über ihre Identität auszuweisen.

2 Der Inhaber der Datensammlung gibt ihr unter Hinweis auf die Angaben gemäss § 14 Absatz 3 Auskunft über alle in der Datensammlung über sie vorhandenen Personendaten.

3 Die Auskunft wird in allgemein verständlicher Form auf Verlangen mündlich oder schriftlich erteilt. Soweit die Mittel und Verfahren des Bearbeitens es zulassen, ist Einsicht in das Register oder in die Personendaten zu gewähren.

4 Kann die Auskunft oder Einsicht der Person selbst nicht gewährt werden, weil sie dadurch zu stark belastet werden könnte oder andere wichtige Gründe dagegen sprechen, kann sie einer Person ihres Vertrauens gewährt werden.

5 Die Kontrollrechte hinsichtlich der in zentralen Datenbanken gespeicherten Personendaten richten sich nach dem Informatikgesetz vom 7. März 2005.

Auf unserer Webseite www.datenschutz.lu.ch unter Publikationen steht überdies kostenlos ein entsprechendes Musterschreiben inkl. Anleitung «Einsicht in die eigenen Daten» zum Download zur Verfügung.

## Handy-Synchronisation in einem Unternehmen mit einem kantonalen Leistungsauftrag

Das Projekt richtet sich an stellensuchende Jugendliche nach Abschluss der obligatorischen Schulzeit, an Lehrstellensuchende oder an Jugendliche, welche die Lehre abgebrochen haben.

Die Kursleiter haben mit der Umstellung von Office 2003 auf 2010 den Wunsch geäussert, dass ihre Termine über ihr privates Handy synchronisiert werden können. Der externe IT-Verantwortliche hat in diesem Zusammenhang darauf hingewiesen, dass mit der Synchronisation nicht nur die Outlooktermine, sondern auch der E-Mailverkehr extern abgerufen werden kann und dies evtl. Fragen betreffend Datenschutz aufwirft.

Mit der Synchronisation sind auch interne Mails auf dem Handy abrufbar. Zum Einloggen wird zwar ein vierstelliges Passwort verwendet, trotzdem besteht die Möglichkeit, dass Dritte sich Zugriff zum Handy verschaffen und so evtl. auch auf interne Daten zugreifen können.

Frage:
Genügt das Einloggen mit dem Passwort?

Fazit:
In der Tat sprechen wir hier auch von BYOD (Bring Your Own Device). Das heisst, private Endgeräte wie Smartphones und Tablets werden für den geschäftlichen Datenverkehr eingesetzt. Dies birgt nicht nur technische Risiken, sondern auch organisatorische bzw. rechtliche Aspekte müssen berücksichtigt werden.

BYOD hat unter anderem folgende organisatorische und rechtliche Aspekte:

1. Data Policy
2. Arbeitsrecht
   a. Einwilligung zu BYOD
   b. Klärung der Eigentumsverhältnisse
   c. Kostenregelung
3. Datensicherheit, Datenschutz und Compliance
4. Immaterialgüterreche und Lizenzrechte
5. Support
6. Haftung

Data Policy:

- Erhebung und Qualifizierung der Daten (werden Personendaten im Sinn des Datenschutzrechts bearbeitet?)
- Wie sensibel bzw. vertraulich ist der Inhalt der E-Mails?

- Daten-Eigentümer bestimmen
- Zugriffsart, -berechtigung (Wer hat wann auf welche Daten Zugriff)
- Speicherort (Wo werden die Daten gespeichert?)
- Ein- und Austrittsprozess (regelmässige Kontrolle der Benutzer- und Zugriffsrechte)

Arbeitsrecht:
- Ohne Einwilligung = erhebliche Rechtsunsicherheit
- Arbeitnehmerreglemente/Nutzungsbedingungen anpassen.
- Hauptverantwortung GL bzw. VR (Art. 716a OR)
- Geheimhaltungsvereinbarung muss von jedem Kursleiter unterschrieben werden
- im Vertragswerk mit den Kursleitern (z.B. in einem Rahmenvertrag) muss ein Hinweis auf die IT-Nutzungsweisung vorhanden sein.

Beim privatem Endgeräte-Eigentum ist das Thema Zugriff auf das Gerät, Remote Wiping und das endgültige zertifizierte Löschen zu klären.

Weiter sind angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten zu ergreifen. Das heisst, das Endgerät muss mind. mit einem 8-stelligen Code vor unbefugtem Zugriff geschützt werden. Dies muss durch eine entsprechende Policy gewährleistet werden und darf/kann vom Benutzer nicht deaktiviert werden können.

Weitere Aspekte betreffen den Bereich Immaterialgüterrechte und Lizenzen:
- Arbeitsresultate gehören dem Arbeitgeber (Art. 322 OR, Art. 17 URG)
- Nebenbeschäftigung von Arbeitnehmern nur mit schriftlicher Bewilligung
- Lizenzen des Unternehmens müssen Privatgebrauch abdecken u.U.

Rechtlicher Lösungsansatz:
- Hauptverantwortung bei VR/GL, kann nicht delegiert werden.
- Überprüfung bestehender Arbeitsverträge/Weisungen/Benutzerreglemente?
- Einwilligung Unternehmen/Mitarbeiter (für Remote Löschung/Backups) vorhanden?

Technische Umsetzung:
- Implementierung von Sicherheitsmassnahmen
- Beschränkung der Zugriffsmöglichkeiten auf Device und Daten
- Entscheid intern / extern (Cloud od. sonst Outsourcing)

Rechtliche Umsetzung: Zusatz Arbeitsvertrag
- Klärung Eigentum Gerät und Daten (inkl. Finanzierungsfrage)
- Verzicht auf Gerät vom Arbeitgeber

Support je nach Benutzer
- Backup- und Verschlüsselungsvorschriften – keine Daten lokal
- Haftungsszenarien/Versicherung
- Remote Wiping bzw. Überschreiben und Zugriffsmöglichkeiten

## 6. Bereich Privat

### Moneyhouse-Einträge

Während des Berichtsjahres haben wir allmonatlich Anfragen von Privaten mit Reklamationen erhalten, welche die Datenverarbeitung von Moneyhouse.ch betreffen. Für die Datenverarbeitung durch Private und durch den Bund ist für die ganze Schweiz der Eidgenössische Datenschutz-

und Öffentlichkeitsbeauftragte (EDÖB) in Bern zuständig (www.edoeb.admin.ch).

Das Unternehmen itonex AG in Rotkreuz betreibt den Internetdienst «Moneyhouse», der umfassende Wirtschaftsinformationen über Firmen und Privatpersonen sammelt, aufbereitet und verwaltet. Diese Informationen sind im Internet zugänglich, teilweise kostenpflichtig, teilweise auch gratis.

Privatpersonen beanstanden, dass «Moneyhouse» ihre Wohnadresse und andere Informationen im Internet publiziert, obwohl sie selber diese bei der Einwohnerkontrolle gesperrt hätten. Andere machen geltend, Informationen aus dem Handelsregister über sie seien nicht mehr aktuell.

Der EDÖB erachtet einige Bereiche von Datenbearbeitungen dieser Firma als unzulässig. Deshalb ist er in den letzten Jahren auch verschiedentlich gegen diese vorgegangen, 2012 auch vor Bundesverwaltungsgericht. Nach vertieften Abklärungen hat der EDÖB eine «Empfehlung» ausgesprochen, welche die Firma itonex AG 2013 akzeptiert hat. Wie Betroffene gegen unzulässige oder unzutreffende Datenbekanntgaben durch «Moneyhouse» vorgehen können, darüber informiert der EDÖB auf seiner Webseite.

## 7. Diverse

### RAV und Jobsuchmaschine «Jobagent.ch»

Aufgrund einer Medienanfrage sowie bereits publizierten Medienberichten zur Praxis von RAV-Stellen in anderen Kantonen war zu prüfen, ob Stellensuchende von ihrem Personalberater bei den RAV-Stellen im Kanton Luzern einen Code für einen zeitlich befristeten und kostenlosen Zugang auf die Onlineplattform «Jobagent.ch» erhalten und dabei die Suchaktivitäten jederzeit durch die Personalberater überwacht werden können.

Dazu stellten sich aus datenschutzrechtlicher Sicht folgende Fragen:

1. Werden die Stellensuchenden über die Einsichtsmöglichkeit durch die Personalberater informiert?
2. Falls die Stellensuchenden über diese Einsichtsmöglichkeit informiert werden, wie und in welchem Umfang erfolgt diese?
3. Welche Personendaten können durch die Personalbera-

ter auf den Profilen der Stellensuchenden von «Jobagent.ch» eingesehen werden (Umfang der technischen Möglichkeit)?

4. Welche Personendaten werden durch die Personalberater auf «Jobagent.ch» tatsächlich eingesehen (Umfang der Datensichtung und -erhebung)?

In der Folge ergab sich, dass die Stellensuchenden durch ihre RAV-Berater bei der Aushändigung des Gutscheins jeweils mündlich auf die Überwachung hingewiesen werden. Zudem wurde seitens der zuständigen Dienststelle Wirtschaft und Arbeit (wira) darauf hingewiesen, dass sich überdies entsprechende Hinweise in den AGB der Plattform «Jobagent.ch» finden liessen, wie dies bei anderen Softwareapplikationen auch der Fall sei. Gleichzeitig bot das wira – was aus Sicht des DSB im vorliegenden Fall unerlässlich und daher zu begrüssen ist, da die bloss mündliche Information wie auch die knappe Erwähnung in den umfangreichen AGB für eine umfassende und damit hinreichende Information der Stellensuchenden nicht genügen – an, ab sofort zusätzlich für jedes RAV proaktiv nachfolgenden Zusatztext zum Datenschutz auf den Gutschein-Codes abzubilden:

Hinweis zum Datenschutz
Nach erfolgter Anmeldung kann Ihr/Ihre Personalberater/in gewisse Informationen einsehen, um gemeinsam Ihre Suchaktivitäten besprechen und optimieren zu können. Es handelt sich dabei um folgende Daten:
– Name, Vorname und E-Mail Adresse
– Anzahl Logins und Datum des letzten Logins
– Gespeicherte Job-Mails

# D. Projekte

Im Berichtsjahr wurden zahlreiche grössere Projekte der kantonalen Verwaltung datenschutzrechtlich begleitet, so unter anderem:

- Pilotprojekt Microsoft O365 an der Kantonsschule Alpenquai Luzern,
- Datenbankanwendung OSIV, welche alle Arbeitsabläufe, die in einer IV-Stelle anfallen, elektronisch abbildet,
- neues Objektwesen Luzern im Rahmen der eGovernment-Strategie des Kantons Luzern,
- SAP-Outsourcing Ausschreibungsstrategie,
- Pilotprojekt «Mein online Spitaldossier»,
- Pilotprojekt «Smarx», welches Kunden mit der Privatwirtschaft und Einwohner mit der öffentlichen Verwaltung im Rahmen der Luzerner eGovernment-Strategie verbindet,
- Einführung einer neuen standardisierten und etablierten IT-Austausch-Plattform für den Versand sensibler Dateien innerhalb der kantonalen Verwaltung,
- Update der IT-Plattform Kompass für die Verwaltung aller kantonalen Lehrbetriebe mit den dazugehörenden Lehrverträgen und Lehrstellen,
- Aufbau eines kantonalen koordinierten Bedrohungsmanagement-Konzepts in den Bereichen Schule, Soziales, Gesundheit, allgemeine Verwaltung und Gerichte,
- Erarbeitung eines übergeordneten Datenschutzreglements für die Luzerner Psychiatrie sowie
- verschiedene weitere Projekte und Vorhaben.

# E. Kontrollen

Im Rahmen unserer aufsichtsrechtlichen Kontrolltätigkeit führten wir im Berichtsjahr einen Audit der Anwendung NEST (LuTax, kantonale Steueranwendung) mit Schwerpunkt «Zugriffsberechtigungen» durch. Dabei wurden Systemdokumentation, Berechtigungskonzept, Admin-Rechte, Zugriff von extern, Vertraulichkeitsvereinbarungen, Benutzer-Mutations-Prozess und die Mitarbeitendenschulung auf Übereinstimmung mit den datenschutzrechtlichen Bestimmungen überprüft. Das Ziel des Audits bestand darin, Verbesserungspotentiale zu erkennen, Sicherheitsmassnahmen zu definieren sowie Schulungsbedarf zu identifizieren. Die Kontrolle ergab erhebliches Verbesserungspotential, welches zu entsprechenden Anpassungsempfehlungen führte.

Aufgrund der herrschenden Ressourcenknappheit lässt sich aber das zur Kontrolle der Einhaltung des Datenschutzes unerlässliche Durchführen von Audits in den Bereichen Informatik, Polizei, Gesundheit, Soziales und Bildung in den Verwaltungen des Kantons (zuzüglich verwaltungsexterne Einheiten mit kantonalen Leistungsaufträgen) sowie der 82 Gemeinden im Zuständigkeitsbereich nicht regelmässig und systematisch umsetzen. Für die Durchführung regelmässiger und systematischer Audits reichen die dem DSB zur Verfügung stehenden personellen und finanziellen Mittel bei weitem nicht aus, so dass entsprechende Kontrollen weder selbst durchgeführt noch extern an spezialisierte Unternehmen (beispielsweise Revisionsgesellschaften) vergeben werden können.

Das Fehlen ausreichender Kontrollmöglichkeiten ist nicht zuletzt auch in Bezug auf die im Rahmen der kantonalen E-Government-Strategie bereits geschaffenen und in den kommenden Jahren noch zu verwirklichenden Webportale und zentralen Datenbanken von Kanton und Gemeinden mit Direktzugriff auf Personendaten problematisch, da in diesem Bereich reelle Gefahren systematischer und mengenmässig umfassender Persönlichkeits verletzungen bestehen. Ebensowenig vermag der Kanton Luzern den Anforderungen des Bundes in Bezug auf die durchzuführenden Kontrollen der Nutzung des Schengen Informationssystems (SIS) durch Polizei und Migrationsbehörden nachzukommen.

# F. Schulungen und Vorträge

Im Berichtsjahr wurden zum Thema Datenschutz und Informationssicherheit verschiedene Schulungen durchgeführt. Zusätzlich wurde dem DSB im Rahmen von Einladungen Gelegenheit geboten, das Thema Datenschutz an der Herbsttagung der Sozialvorsteher des Kantons Luzern vorzutragen, dem Austausch- und Koordinationsgremium des E-Government Forums Luzern ein Referat zum Thema «Datenschutz und Cloudlösungen» zu halten und das neue kommunale Datenschutz-Reglement in der Gemeinde Meggen vorzustellen.

Aufgrund der herrschenden Ressourcenknappheit lässt sich die erforderliche proaktive Sensibilisierung und Schulung der Gemeinde- und Kantonsmitarbeitenden allerdings nicht umsetzen. Schulungen und Vorträge konnten daher lediglich auf Anfrage hin abgehalten werden.

# G. Datenschutz- und Sicherheitstipps

## 1. Aktiver Schutz

### So sperren Sie Ihre Daten im Internet als Liegenschaftseigentümer

Wenn Sie Eigentümerin oder Eigentümer einer Liegenschaft (Wohnung oder Haus) sind, sind heute Ihre Eigentümer-Informationen weltweit im Internet abrufbar. Neben den Angaben zu Ihren Grundstücken veröffentlichen viele Gemeinden in den entsprechenden Informations-Blättern und Webseiten auch Namen und Adresse aller Grundeigentümer im Internet.

Wenn Sie dies nicht wünschen, können Sie beim Grundbuchamt und bei der Gemeinde verlangen, dass Ihr Name im Internet gesperrt wird.

### So können Sie Ihre Auto-Nummer sperren lassen

Fahrzeughalterdaten, welche vom Strassenverkehrsamt Luzern verwaltet werden, sind für jedermann im Internet zugänglich. Die gesetzliche Grundlage für diese Veröffentlichung befindet sich in Art. 104 Abs. 5 Strassenverkehrsgesetz vom 19. Dezember 1958. Diese Bestimmung wird für die Bekanntgabe von Personendaten der Fahrzeughalter durch Art. 126 Verordnung vom 27. Oktober 1976 über die Zulassung von Personen und Fahrzeugen zum Strassenverkehr ergänzt. Die Eidgenössische Datenschutzkommission hat am 22. Mai 2003 entschieden, dass es für die Sperrung der Bekanntgabe von Fahrzeughalterdaten genügt, wenn eine Person glaubhaft macht, dass sie sich einem Risiko oder dem Ungemach der Neugierde nicht ausgesetzt sehen will. Ein konkreterer Beweis oder Indizien für die befürchteten Risiken dürfen von der kantonalen Behörde nicht verlangt werden. Ein entsprechendes Gesuch für die Sperrung von Fahrzeughalterdaten finden Sie auf der Webseite des Strassenverkehrsamtes (www.strassenverkehrsamt.lu.ch).

## 2. BYOD – «Bring Your Own Device»

Zahlreiche Sicherheitsherausforderungen für die öffentliche Verwaltung und Unternehmen:
BYOD hat bestehende Sicherheitsbedenken gegenüber mobilen Endgeräten zusätzlich vergrössert, zudem bringt der Massenkonsum entsprechender Geräte im Kanton Luzern oder in Unternehmen neue Sorgen mit sich, die IT-Profis und Anwender gleichermassen betreffen. Durch die Verwendung mobiler Endgeräte müssen die entsprechenden IT-Weisungen und die zugehörigen Prozesse überarbeitet werden. Aber was sind die grössten Bedenken im Hinblick auf die persönlichen Smartphones und Tablets der Mitarbeitenden?

Folgende Sicherheitsrisiken müssen neu bewertet und im Detail betrachtet werden:

- Datenverlust,
- Konformität,
- Bedienbarkeit,
- Nutzungsbedingungen (Weisungen),
- Vertraulichkeit in Bezug auf das Amtsgeheimnis,
- persönliche Daten und Privatsphäre (Datenschutz),
- gewillte Datenlöschung,
- Standardisierung,
- Unterhalt und Support,
- Eigentumsverhältnisse,
- Software-Lizenzen,
- Zugriffsberechtigungen,
- Speicherort der Daten etc.

Wenn Sie die Benutzung mobiler Geräte unterstützen oder dies planen, dann sollten Sie sich über nachfolgende Sicherheitsprobleme Gedanken machen. Wir zeigen Ihnen auch, wie Sie die Herausforderungen adressieren können.

## Sicherheitsrisiken

In der Vergangenheit hat die IT-Abteilung den Mitarbeitenden nur «Enterprise-ready»-Smartphones angeboten. Diese galten als sicher, liessen sich gut verwalten und wurden den Business-Ansprüchen gerecht. Heutzutage sorgen sich IT-Profis, dass die persönlichen Consumer-Smartphones und -Tablets der Mitarbeitenden existierenden Weisungen nicht gerecht zu werden vermögen.

Die IT-Abteilung kann allerdings gewisse Kriterien aufstellen und persönliche Geräte akzeptieren, die für das Business geeignet sind. Beispiele wären Geräte-Typ und Version des Betriebssystems. Sie sind nicht glücklich über Geräte mit Android 4.1 oder iOS? Blockieren Sie den Netzwerkzugriff sowie System- und Datenzugriffe für diese. Besser wäre noch eine Weisung, die als riskanter eingestuften Geräten den Zugriff begrenzt, zum Beispiel in Form virtualisierter Interaktion mit Firmen-E-Mails über eine Terminal-Server Lösung.

## Datenverlust

Fakt ist, dass mobile Geräte leicht verloren gehen oder gestohlen werden. Ist solchen Geräten der Zugriff auf das Firmennetzwerk oder auf Unternehmenssysteme und -daten gestattet, sind sie in den falschen Händen ein grosses Problem. Aber selbst Consumer-Geräte verfügen heutzutage über Mechanismen, um diese Probleme zu adressieren. Dazu gehören Passwort-Sperren, Verschlüsselung und Fernlöschen (Remote Wipe) von Daten. Nichtsdestotrotz sollte die IT-Abteilung sicherstellen, dass die Anwender von diesen Features auch Gebrauch machen.

Zum Glück gibt es viele Tools, mit denen IT-Abteilungen die oben genannten Funktionen kontrollieren können. Unternehmen können mithilfe von Microsoft ActiveSync-Policies sicherstellen, dass nur Anwender Zugriff von ihrem mobilen Gerät auf die Firmen-E-Mails haben, die auch Passwörter und eine Verschlüsselung verwenden. Ebenso lässt sich ein Fernlöschen erzwingen. Stellen Unternehmen höhere Ansprüche, können sie Mobile Device Management- (MDM-)Systeme einsetzen. Anwender würde man dann beispielsweise auffordern, ihre Geräte durch diese MDM-Systeme verwalten zu lassen. Damit ist ein Automatisieren und Aktualisieren der Security Policies möglich.

## Konformität

Selbst durch einfachen Schutz vor Datenverlust kann das Sicherstellen der Konformität mit den von der IT-Abteilung definierten Security Policies zu einer Herausforderung werden. Ohne permanentes Monitoring ändern Mitarbeitende vielleicht aus Bequemlichkeit die Passwörter oder die Timeouts bei Inaktivität. Möglicherweise entfernen sie noch andere von den IT-Abteilungen ausgegebene Beschränkungen, wie zum Beispiel das Installieren von Applikationen aus inoffiziellen Quellen. Anwender installieren oft massenweise Software von Drittanbietern auf ihren Geräten. Somit schleicht sich möglicherweise Adware oder Malware ein. Dies ist natürlich ein Risiko für Firmennetzwerk, -server und -daten.

Um die Konformität auf den Anwender-Geräten überprüfen zu können, müssen Sie natürlich Einblicke bezüglich Einstellungen, Applikationen und Aktivitäten haben. Setzen Firmen MDM-Lösungen ein, können sie dies realisieren und die Einhaltung der Regeln erzwingen.

Zum Beispiel können viele MDM-Tools in regelmässigen Abständen die installierten Applikationen abfragen. Somit stellt man sicher, dass benötigte Anwendungen installiert bleiben und andere keine Malware enthalten. Sollte ein Gerät als nicht mehr konform angesehen werden, sorgen die MDM-Tools für einen Ausschluss und verwehren den

Zugriff auf das Firmennetzwerk. Dem Anwender können sie sogar eine Nachricht hinterlassen, wenn er eine Deinstallation von Enterprise-Applikationen versucht. Eine Änderung der Netzwerkeinstellungen ist ebenfalls möglich, um das Gerät in eine digitale Quarantäne zu sperren.

### Persönliche Daten und Privatsphäre (Datenschutz)

Die Mitarbeitenden stimmen den Auflagen seitens der IT-Abteilung möglicherweise zu. Allerdings machen sie sich sicher Gedanken über die Integrität ihrer persönlichen Daten. Dazu gehören Fotos, Musik, Kontakte und Applikationen.

Um dieses Problem zu adressieren, können moderne MDM-Lösungen persönliche und geschäftliche Daten auf den Geräten der Anwender besser separieren. Die IT-Abteilung hat somit eine strenge Kontrolle hinsichtlich der Sicherheit von Geschäftsdaten, ohne den persönlichen Informationen zu Nahe zu kommen. Zum Beispiel unterstützen die meisten MDM-Tools ein so genanntes «Enterprise Wipe». Dies löscht lediglich durch MDM-Systeme verursachte Einstellungen und Applikationen, anstatt alles auf dem Gerät auszuradieren. Alternativ könnte die IT-Abteilung Enterprise-Daten in einen speziellen und verschlüsselten Daten-Container legen. Dieser liesse sich dann ohne Zustimmung des Anwenders deaktivieren oder löschen.

Sowohl der Arbeitgeber als auch Arbeitnehmer haben sicherlich Vorbehalte, inwieweit die Sicherheits-Massnahmen in die Privatsphäre der Anwender eingreifen. Einige Menschen finden mit Sicherheit das permanente Monitoring der Geräte als zu aufdringlich. Dazu gehören das Protokollieren persönlicher Kommunikation oder wo sich der Anwender ausserhalb der Geschäftszeiten aufhält.

Einige Arbeitgeber adressieren diese Bedenken mithilfe von Security-Weisungen in Bezug auf Mobilgeräte. Sie führen detailliert auf, auf welche Weise die IT-Abteilung die gesammelten Informationen verwenden kann oder eben nicht. Die bessere Option ist die, Sicherheits-Massnahmen zu limitieren. Zum Beispiel könnte man die Standortüberwachung erst dann aktivieren, wenn das Gerät als gestohlen gemeldet wurde. IT-Abteilungen sollten in der Regel von einer Protokollierung Abstand nehmen, ausser es ist unbedingt für das Business notwendig. Mehr und mehr Firmen akzeptieren Bring Your Own Device (BYOD). Somit sollten sich IT-Abteilungen die hier genannten Schritte und Tipps zu Herzen nehmen, um die grössten Sicherheitsbedenken aus der Welt zu schaffen. Im Laufe der Zeit entwickeln sich sowohl die Geräte als auch die Anforderungen weiter. Das sollte auch für die Herangehensweise hinsichtlich Mobile Security der Fall sein.

# H. privatim

Der Kanton Luzern ist Mitglied des Vereins privatim. Dieser Verein bezweckt eine interkantonale Zusammenarbeit im Bereich des Datenschutzes, damit die Mitglieder (vorwiegend kantonale DSB), die allesamt über beschränkte Mittel verfügen, gewisse Arbeiten effizienter bewältigen bzw. aufteilen können.

Die Arbeitsgruppe «Schule» hat sich im Berichtsjahr mit verschiedenen datenschutzrechtlichen Themen im Bereich Schule befasst und verschiedene Merkblätter im Zusammenhang mit Schule und IT erstellt. Der DSB ist Mitglied der Arbeitsgruppe «Schule».

Die Arbeitsgruppe «ICT» beschäftigte sich im Berichtsjahr mit den Themen E-Mail Verschlüsselung und BYOD (Bring Your Own Device). Der Mitarbeiter des DSB, Wolfgang Sidler, ist Mitglied der Arbeitsgruppe «ICT».

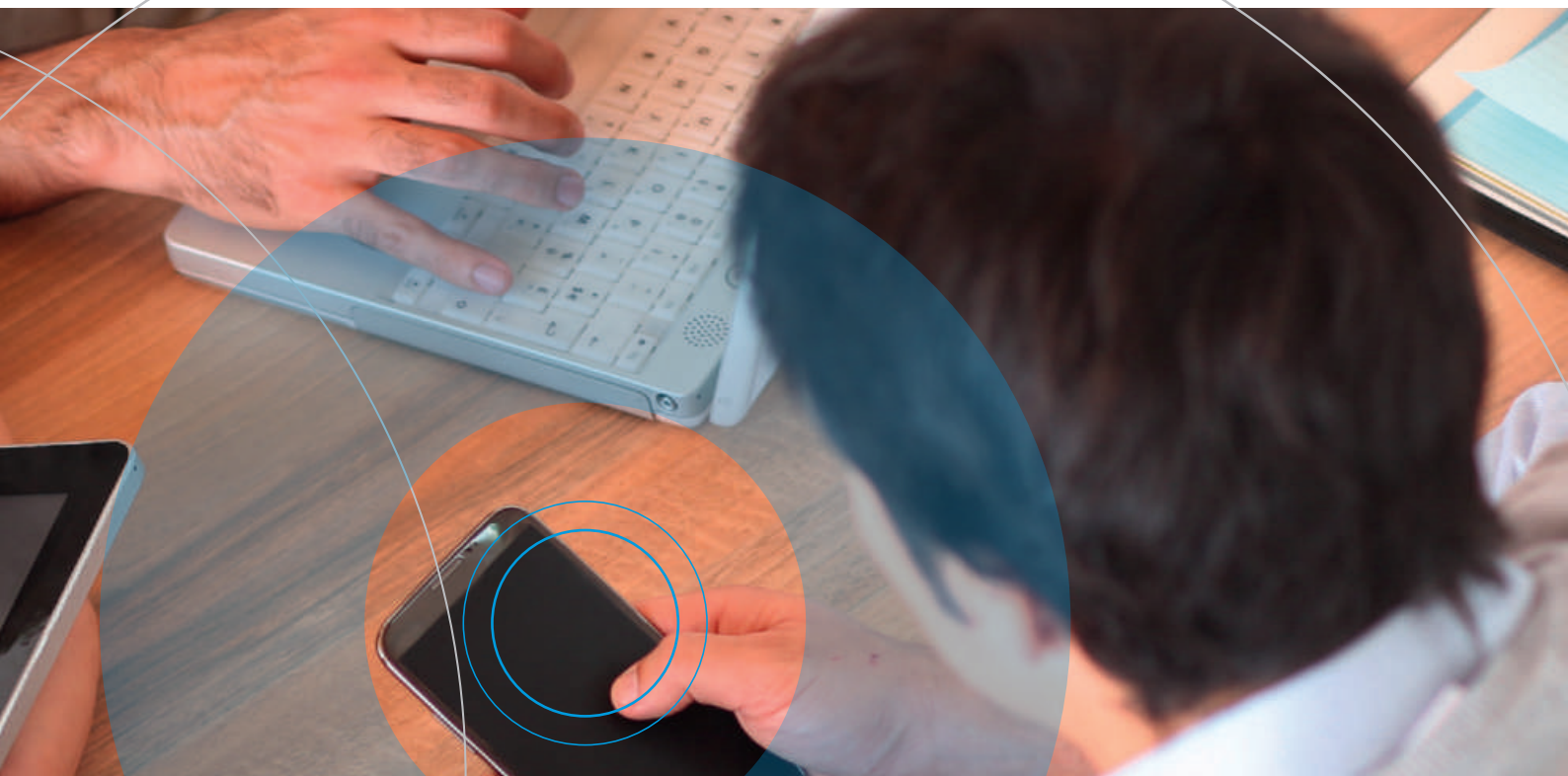
Privatim führt zwei Mal jährlich ein Plenum durch, bei dem sich die Mitglieder zwecks Besprechung von und Austausch in aktuellen Datenschutzfragen treffen. Diese Veranstaltungen werden abwechslungsweise durch die einzelnen Mitglieder organisiert und fanden im Berichtsjahr in Lausanne und Frauenfeld statt.

# I. Webseite www.datenschutz.lu.ch

Die Webseite enthält verschiedene inhaltlich gegliederte Rubriken. Sie verweist auf die wichtigsten Rechtsgrundlagen im Bundes- und kantonalen Recht. Folgende Themen werden speziell bearbeitet und in Form von Merkblättern aktualisiert: Schulen, Gesundheitswesen, Informatik, Videoüberwachung, Polizei und Diverses. Der Besucher kann auch Formulare, Checklisten und andere hilfreiche Unterlagen herunterladen. Zudem werden die Publikationen des DSB auf der Webseite veröffentlicht. Schliesslich wird auch die Möglichkeit angeboten, dem Unterzeichnenden über das Kontaktformular Fragen zu stellen.

Die Kennzahlen der Besucher-Analyse zeigen auf, wie unsere Datenschutz-Webseite www.datenschutz.lu.ch besucht wurde. Die Zahlen zeigen, dass das Bedürfnis einer Datenschutz-Webseite ausgewiesen ist. Der DSB hätte zwischen Januar und Dezember 2013 nie die entsprechenden Fragen beantworten können, wenn die interessierten Personen angerufen hätten, statt auf die Webseite zu gehen.

| **Dienstleistungen** | 2010 | 2011 | 2012 | **2013** | Entwicklung (2012 – 2013) |
|---|---|---|---|---|---|
| Besucher Insgesamt | 3'189 | 2'788 | 2'946 | **3'211** | + 9% |
| Besucher pro Tag | 8 | 7 | 8 | **9** | |
| Seitenansichten Insgesamt | 10'560 | 7'190 | 7'877 | **8'850** | + 12% |
| Seitenansichten pro Tag | 28 | 19 | 21 | **24** | |



# J. Medienarbeit

Im Berichtsjahr erhielt der DSB insgesamt 37 Medienanfragen zu folgenden Themen:

- Datenaustausch Asylwesen,
- Internetpranger einer Jungpartei,
- Videoüberwachung durch ein Oberstufenzentrum,
- Veröffentlichung Labordaten,
- öV-Karte,
- Vorermittlungsdatenbank,
- Aktenvernichtung Kinder- und andere Heime,
- Videoüberwachung Banken,
- Videoüberwachung öffentlicher Raum,
- Pilotprojekt «Mein online Spitaldossier»
- Google Streetview im Kanton Luzern,
- Internetfahndung,
- Datenspeicherung Smartphone,
- Auswirkung NSA-Abhörskandal auf die Zentralschweiz,
- Nutzung Facebook durch Schulen,
- Microsoft Office365 im Schulbereich,
- Cloud Computing in der kantonalen Verwaltung,
- RAV-Kooperation mit Plattform «jobagent.ch»,
- Datensicherheit in der Verwaltung,
- Prüfungsergebnisse Dritte abrufbar im Intranet eines Hochschuldepartements,
- Drohneneinsatz Polizei zur Überwachung von Fussballfans,
- Forschungsprojekt: Fotografieren von Passanten,
- Datenweitergabe Sportveranstaltung,
- Videoüberwachung Unterrichtsräume Uni Luzern,
- E-Mail Kommunikation Kantonsverwaltung mit Bürgerinnen und Bürgern,
- Familienforschung.

Aufgrund der geringen personellen Ressourcen ist jedoch nicht an eine umfassende und proaktive Informationspolitik seitens des DSB zu denken. Dies ist problematisch, da die Information der Bevölkerung auch zu den Aufgaben des DSB gehört, was die europäischen Instanzen im Rahmen der Überprüfung der Datenschutztätigkeiten in der Schweiz unterstrichen und deren Umsetzung gleichzeitig bemängelt haben.

# K. Ausblick

Neben neuen technischen Herausforderungen wie «Big-Data», «Dash-Cams in Fahrzeugen» oder «Google-Glass», die zumindest in naher Zukunft auch bei kantonalen und kommunalen Verwaltungsstellen in der einen oder anderen Form zur Diskussion stehen dürften, werden auch seit Jahren aktuelle Themen wie beispielsweise der Einsatz von «Drohnen», Videoüberwachungen, die Umsetzung der kantonalen «E-Government-Strategie» sowie «Cloud Computing» und «BYOD» in der Verwaltung den DSB und dessen Mitarbeiter weiterhin mit interessanten Anforderungen, Projekten und Fragestellungen aktiv und umfassend beschäftigen.

Die aktuellen rechtlichen, technischen und gesellschaftlichen Entwicklungen wirken sich direkt auf die öffentlichen Verwaltungen im Kanton Luzern aus und erfordern künftig auch vermehrte sowie umfassendere Beratungs-, Schulungs- und Kontrollkapazitäten seitens des Datenschutzes. Dies ist unerlässlich, um den gesteigerten Anforderungen der Behörden sowie Bürgerinnen und Bürgern nachkommen zu können.

Die Erfüllung dieser jährlich gestiegenen und sich auch künftig aufgrund der zunehmenden technischen und gesellschaftlichen Komplexität weiter steigenden Anforderungen an den Datenschutz und damit auch an die Datenschutzaufsicht, hängt zum einen von ausreichenden finanziellen Ressourcen sowohl in Bezug auf Personal- wie Sachmittel ab. Diesbezüglich ist die Datenschutzaufsicht des Kantons Luzern auch im Vergleich zu den anderen Kantonen sehr schlecht ausgestattet.

Abgesehen von der für die Erfüllung der gesetzlichen Aufgaben der Datenschutzaufsicht erforderlichen Verbesserung der Mittelausstattung, sind auch organisatorische Anpassungen zur Gewährleistung der Unabhängigkeit erforderlich, sei dies durch Wahl des DSB auf feste Amtsdauer wie auch durch Einräumung finanz- und personalrechtlicher Kompetenzen an den DSB analog dem Entwurf zum Mantelerlass Anlaufstelle in Verwaltungsangelegenheiten, der soeben in Vernehmlassung war, und direkten Zugang zum Kantonsrat in Budgetangelegenheiten sowie personalrechtliche Selbständigkeit vorsieht. Es handelt sich dabei um Anliegen, die in Bezug auf die Datenschutzaufsicht im Kanton Luzern bislang nicht umgesetzt werden konnten, was in Bezug auf die Unabhängigkeit problematisch ist.

Es bleibt daher zu hoffen, dass die Auswirkungen der rechtlichen, technischen und gesellschaftlichen Entwicklungen auf den Datenschutz im Kanton Luzern erkannt und die dazu notwendigen finanziellen, rechtlichen und organisatorischen Anpassungen zeitnah umgesetzt werden.

## Adressen

Datenschutzbeauftragter
des Kantons Luzern
Murbacherstrasse 21
6002 Luzern
Telefon 041 228 66 06
datenschutz@lu.ch
www.datenschutz.lu.ch

Eidgenössischer Datenschutz-
und Öffentlichkeitsbeauftragter
Feldeggweg 1
Postfach
3003 Bern
Tel. 031 322 43 95
www.edoeb.admin.ch

## Nützliche Websites anderer Kantone oder Vereinigungen

www.baselland.ch/datenschutz
www.datenschutz-zug.ch
www.datenschutz.ch
www.privatim.ch

900145 diekonkreten.ch

KANTON LUZERN

**Datenschutzbeauftragter**
Murbacherstrasse 21
6002 Luzern